Secure Shell (SSH) Protocol

The Secure Shell (SSH) protocol provides secure, encrypted communication between two untrusted hosts over an unsecured network, requiring users to prove their identities to successfully connect to a remote system. SSH is used both for interactive login sessions and for executing arbitrary commands on remote systems. Authentication information, such as a password or passcode, as well as data are both encrypted over the network.

SSH uses a client-server model. On the client, you initiate an SSH connection with the **`ssh`** command, which connects to the **`sshd`** daemon on the remote system.

OpenSSH at NAS

All NAS systems use the OpenSSH implementation of the SSH protocol. This implementation includes **`ssh, scp, sftp, sshd,`** and utilities such as **`ssh-add, ssh-agent,`** and **`ssh-keygen`**. Although OpenSSH includes support for both the SSH-1 and SSH-2 protocols, NAS systems accept connections using SSH-2 only.

WARNING: Due to security and performance issues with older versions of OpenSSH, we strongly recommend that you use OpenSSH 5.2 or later for best performance, security, and functionality.

Operating System Considerations

MacOS and Linux

MacOS and most Linux distributions include a version of OpenSSH. However, it is important to keep up with the latest security updates for your operating system to ensure that you have the latest version of OpenSSH supported by the vendor.

Windows/Cygwin

On systems running the Windows operating system, you must install a client that supports the SSH-2 protocol.

We recommend using Cygwin, which provides a Linux-like environment for Windows, and OpenSSH. For download and installation instructions, see Installing Cygwin (PDF).

Note: By default, Cygwin does not support the new and improved SSH encryption ciphers used at NAS. To enable SSH connections, add the following lines to your **`~/.ssh/config file`**:

```
Host *
    KexAlgorithms +diffie-hellman-group1-sha1
```

To learn more about OpenSSH, see the **ssh(1)** and **ssh_config(5)** man pages.

See the following Wikipedia pages for more information:

- Secure Shell
- OpenSSH
- Cygwin

Article ID: 228
Last updated: 21 Jul, 2020
Revision: 18
Security and Policies -> Security -> Secure Shell (SSH) Protocol
https://www.nas.nasa.gov/hecc/support/kb/entry/228/